

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表平6-501571

(43) 公表日 平成6年(1994)2月17日

第6部門第2区分

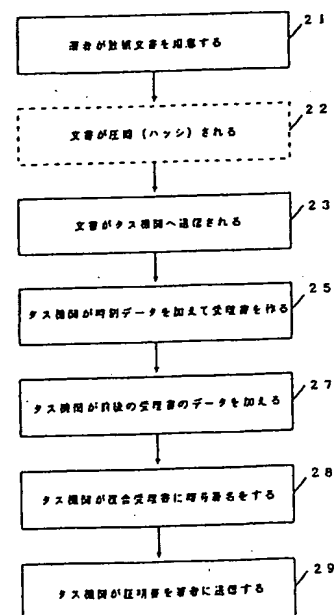
(51) Int.Cl. <sup>3</sup>	識別記号	庁内整理番号	F I
G 0 9 C 1/00		9194-5L	
H 0 4 L 9/32		7117-5K	H 0 4 L 9/ 00
			A
審査請求 有 予備審査請求 有 (全 10 頁)			
(21) 出願番号	特願平3-516026	(71) 出願人	ベル コミュニケーションズ リサーチ インコーポレーテッド
(86) (22) 出願日	平成3年(1991)7月30日		アメリカ合衆国、07039-2729 ニュージ ャージー州、リビングストン、ウエスト マウント プレザント アベニュー 290
(85) 翻訳文提出日	平成5年(1993)2月2日	(72) 発明者	ハバー、スチュアート、アラン
(86) 国際出願番号	P C T / U S 9 1 / 0 5 3 8 6		アメリカ合衆国、10003 ニューヨーク州、 ニューヨーク、アービン プレイス 22、 アパートメント 2 シー
(87) 国際公開番号	W O 9 2 / 0 3 0 0 0	(74) 代理人	弁理士 小林 孝次
(87) 国際公開日	平成4年(1992)2月20日		
(31) 優先権主張番号	5 6 1, 8 8 8		
(32) 優先日	1990年8月2日		
(33) 優先権主張国	米国 (U S)		
(31) 優先権主張番号	6 6 6, 8 9 6		
(32) 優先日	1991年3月8日		
(33) 優先権主張国	米国 (U S)		

最終頁に続く

(54) 【発明の名称】 数値文書にタイムスタンプを確実に押す方法

## (57) 【要約】

文字数字式やビデオやオーディオや絵のデータを含む、数値文書にタイムスタンプを押すシステムは文書テキストの秘密を守り、その文書が成立した時刻に対する著者の主張を確立する、不正変改の恐れのない時刻のシールを提供します。最初に、文書は一方方向性のハッシュ関数で一つの数字に圧縮され、これによって文書テキストの独自の表示を確定するかも知れません。本発明の一実施例ではこの数字はそれから外部機関に送信され、そこでその時の時刻が加えられて受理書が作られ、これが公開鍵署名法で機関によって証明されて、文書存在の証拠として著者に返されます。機関によるタイムスタンプに通謀による不正がないようにし、システムの信頼性を高めるために、受理書は他の同じ頃の受理書と結合され、かくして連続の時の流れの中の文書の位置を確定してから、機関によって証明されます。他の実施例では、タイムスタンプされる文書のハッシュ数の関数を独自の種として、これによる無作為選択によって複数の機関が指定されます。もう一つの実施例では、機関は受理書のデータにその時の記録連鎖証明書を加えてハッシュして受理書を



特許請求の範囲

証明します。ここでその時の記録連鎖証明書は前の受理書の夫々をその時々々の連鎖証明書と次々にハッシュした結果得られる数です。文書の存在を後で証明するには、機関の公開の鍵を使い、問題の文書の表示を使って証明の段階を繰り返して、証明書の真正であることが認証されます。問題の文書が原文書と同一である時だけ両方の証明書の数が一致します。

1. a) 数値文書の数値表示が制作者から外部機関へ送達され、  
b) この外部機関がこの数値文書の数値表示の少なくとも一部分とその時の時刻の数値表示とを包含する受理書を作り、  
c) この受理書がこの外部機関によって証明できる数値署名法によって証明されることを特徴とする数値文書にタイムスタンプを密着に押す方法。
2. 前記数値文書表示受理書が前記数値文書に決定関数法を適用して得られる数の数値表示の少なくとも一部分を包含する前記特許請求の範囲第1項記載の方法。
3. 前記数値数値表示が前記数値文書に一方向きハッシュ法を適用して得られる前記特許請求の範囲第2項記載の方法。
4. 前記受理書が前記外部機関が受理した他の数値文書の少なくとも一つに特有な時刻表示と数値文書表示とを更に包含する前記特許請求の範囲第1項記載の方法。
5. 前記外部機関が予め定められた世界から、前記数値文書に決定関数法を適用して得られる数の数値表示の少なくとも一部分を基として疑似無作為生成機で無作為に、選ばれる前記特許請求の範囲第1項記載の方法。
6. 前記疑似無作為生成の値が前記数値文書に一方向きハッシュ法を適用して得られる前記特許請求の範囲第5項記載の方法。
7. 前記疑似無作為生成によって選ばれた少なくとももう一つの付加的な外部機関によって同時にタイムスタンプ証明書が作られる前記特許請求の範囲第5項記載の方法。

8. 前記疑似無作為生成によって選ばれた少なくとももう一つの付加的な外部機関によって同時にタイムスタンプ証明書が作られ、夫々の付加的な外部機関の選択時の入力値は以前に作られた出力の数値表示に前記一方向きハッシュ法を適用して得られる出力の数値表示の少なくとも一部分である、前記特許請求の範囲第7項記載の方法。

9. a) 一つのシリーズの文書の特定の一つの数値表示を作り、

b) 前記特定文書表示と前記シリーズ中の前記特定文書の直前の文書に対する証明書記数連鎖数値表示を包含する連鎖に対して決定関数法を適用して前記特定文書に対する証明書記数連鎖数値表示を作る

ことを特徴とする一つのシリーズの数値文書の時刻的順序を証明する方法。

10. 前記シリーズの以後の文書の夫々に対して前記の段階を繰り返すことを更に包含する前記特許請求の範囲第9項記載の方法。

11. 前記文書表示の夫々が前記文書に決定関数法を適用して得られる前記特許請求の範囲第10項記載の方法。

12. 数値文書の数値表示を外部機関に送達し、前記外部機関がこの時の時刻の数値表示と前記数値文書の数値表示の少なくとも一部分を包含する受理書を作り、前記外部機関で前記受理書を証明する時、

a) 前記受理書の数値表示を以前の証明書記数連鎖の表示と連関して複合表示を作り、

b) 前記複合表示に決定関数法を適用して前記受理書に対する証明書記数連鎖を作る

5

ことによって前記受理書を証明することを特徴とする数値文書にタイムスタンプを押す方法。

13. 前記外部機関がこれ迄のタイムスタンプ処理の証明書記数連鎖を包含する記録を保持する前記特許請求の範囲第12項記載の数値文書にタイムスタンプを押す方法。

14. 前記受理書に含まれる数値文書表示が前記数値文書に決定関数法を適用して得られる数の数値表示の少なくとも一部分を包含する前記特許請求の範囲第12項記載の数値文書にタイムスタンプを押す方法。

15. 前記数値表示が前記数値文書に一方向きハッシュ法を適用して得られる前記特許請求の範囲第14項記載の数値文書にタイムスタンプを押す方法。

## 明 細 書

## 数値文書にタイムスタンプを確実に押す方法

## 発明の背景

文書が与えられた日付を立証し、問題の文書の内容が日付の押された原文書の内容と実際に同じであることを証明することが多くの場合に必要です。例えば、知的財産に関しては、ある人が発明の内容を最初に記録した日付を立証することは極めて重要です。発明の考えをタイムスタンプする普通のやり方は、研究室の記録簿に自分の仕事を毎日書き込むことです。閉鎖的に日付を書きつけて署名した記録が記録簿の各ページに次々と書き込まれ、誤り番号を打たれて送られたページは記録を消さないように変更することを困難にします。記録の正確性は、一般に利害関係のない第三者によって定期的に検閲され証人として署名されることによって、更に高められます。何年かたかということが後で証明されなければいけなくなった時、記録簿の物理的な内容と定められた記録の手段の両方が、少なくとも記録簿の証人の日付の時には考えが存在していたという事実を立証する効果的な証拠となります。

同じことのできるテキストの数値的な表示だけでなく、ビデオやオーディオや他のデータを含む、電子文書が数々と広く使われるようになって来て、このような文書の日付を確立する「記録簿」の概念の適用可能性が争われています。電子数値文書は極めて容易に改訂され、このような改訂は後に証拠を偽造するので、ある文書が作られた日付を本当にその文書が示しているのか、又元来のメッセージを今でも本当に表しているのかについて

ついて両者の証拠を提供しますが、このメッセージの受取人だけが、メッセージは受取った時刻以前に存在したことを知る事ができますから、この問題は今でもあります。しかし、このような受取はメッセージが存在した時刻の正確な証拠を全世界に提供はしません。受取ったメッセージに関連する受取人の証言はメッセージの内容とその存在の時刻についての証拠を提供しますが、このような証拠は電子数値文書の内容が、送信者または証人によって簡単に改訂できるという基本的な問題を抱えています。

従って、送る文書が簡単に改訂できる数値形式で書かれる世界になるという予想は、このような文書の信頼性を確立する既存の手段を本質的に危うくします。数値文書の内容と時刻を確定し、少なくとも有形文書の場合に現在認められている程度に、内容と時刻に関して正確な証拠を提供することができるような立証のシステムが現在明白に確立に必要とされています。

## 発明の概要

この発明は数値文書をタイムスタンプする方法において信頼できるシステムを作り、現在の記録簿の本質的な特徴の二つと同等のものを提供します。第一に、文書の内容とその存在のタイムスタンプは、文書の数値データに消えないように記録され、これによって出来たタイムスタンプされたデータのいかなる部分も、改訂が明白とならないように改訂することは不可能であります。このように、文書のテキストの状態はタイムスタンプの瞬間に確定されます。第二に、数値文書がタイムスタンプされた時刻は、虚偽の時刻の表現を記録することを防ぐ、数値的に「証人として」署名する手順で確定されます。基本的に、この方法はタイムスタンプの適用のコントロールを著者から独立機関へと移し、其の時刻以外のス

は、信頼できる証拠は限られています。同じ理由で、立証する署名の信頼性についても重大な疑いが生じます。数値文書の内容の改訂を許さない効果的な手段がないと、システムの信頼性が基本的に欠けていることは電子文書の有効性がもつと広く採用されることを妨げます。

現在でも、電子文書の送信を確証する若干の手段があります。しかし、実際にはこのような手段は両方向の通信に限られます。即ち、このような通信では、送信者は送信される文書の元来の内容と受信者を受信者に立証しようと本質的に望みます。例えば、「秘密の鍵」を使う暗号法は長い間、限られた数の、お互いに知合っていて暗号を解く鍵を知っている個人の間で、メッセージの送信に使われてきました。メッセージを暗号にすることは不正交差を防ぎ、秘密の鍵を使うと送信されたメッセージの「平文」が得られると言う事実が、メッセージは決まったグループの一人が送信したものである証拠となります。しかし、メッセージを書いた時刻は間接的に、受信者が受取った時刻より後ではないと、証明されるに過ぎません。それで、この方法は限られない世界で使われて役に立つタイムスタンプの証拠を生成しません。

もつと広く適用される立証通信法、即ち「公開の鍵」を使う暗号法が、ディフィーとヘルマン（「暗号法の新しい方向」、IEEE 情報理論雑誌、第17-22巻、昭和51年11月、644-654ページ）によって記述され、その後リベスタ等によって、昭和58年9月20日付のアメリカ合衆国特許4,405,829号で実行されました。この方法は利用者の世界を、公表された名簿以外ではお互いに未知の、実質上限定されない数のシステム加入者に拡大しましたが、立証できる通信は依然として両方向のものでした。送信者の秘密の鍵で暗号化されたメッセージの公開の鍵での解読を伴うもののような、公開の鍵の「署名」は、限定されない世界のどのメンバーにもメッセージの送信者が確かに

スタンプをするよう機関に影響を及ぼす能力を著者から取上げます。

この発明の方法は、文書の著者が通信網の中に沢山散らばっていると仮定します。このような著者は個人、会社、会社の部門等で、夫々が区別され、証言番号等で特定できる、著者世界の一人です。この発明の一つの実施例では、この世界はタイムスタンプ機関（タス機関）の依頼人で構成されます。もう一つの実施例では、散らばった著者の夫々がこの世界の他のメンバーの為にタイムスタンプのサービスを行う機関であります。

一般の適用においては、図面の第1図に示されるように、この方法では、著者が広く文字、数字、音声、画面の表示を含む数値文書を作成し、この文書を、并みしくは圧縮した形で、タス機関へ送信します。タス機関は受理した時刻を表す数値データを加えて文書にタイムスタンプし、この文書にその機関の署名を入れて暗号化し、できた文書即ち原文書の存在時刻証明書を著者に返信し、著者はこのような存在を証明することが必要になる時の為に保管します。他の方法では、タス機関は受理した時刻を表す数値データを加えて文書にタイムスタンプし、受理書を作ります。これまでの受理書を暗号化しただけのものにこの受理書を添付し、この数値文書から以下に詳述する決定関数を使って新しい数値文書を作ります。これによってできた数値文書を時刻その他の記録データと一緒に証明書を作ります。

タス機関への通信中に秘密文書の情報が盗取されるのを防ぐために、また全文書の送信に要する数値帯幅を減らすために、著者は場合によっては数値文書の一層を決定関数を使って数値のサイズを大幅に圧縮して独自の鍵に交換するかも知れません。決定関数としては、例えば専門分野では「一方向性ハッシュ関数」として知られる多数のアルゴリズムのどの一つでも使えます。ハッシュ関数のこのような応用は、例えばダムガードによって文書

署名法における安全改良の議論の中で述べられています（「衝突のないハッシュ関数と公開鍵を使う署名法」、暗号学の進歩—ニューロクリプト1987、スプリングー・フェルラー、LNCS、1988、第304巻、203—217ページ）。しかし、この発明の応用では、ハッシング法に真実的な「方向」性はもう一つの目的に叶います。すなわち、タス関数がタイムスタンプを付したり、文書を連署証明書に編み込んだ後では、文書は密かに改変されることはできないという保証を提供します。

ハッシング関数は丁度このような保証を提供します。というのは、著者の署名や合意連署処理済の文書がハッシュされる時に元の内容の代表的な「指紋」が作られ、これから元の文書を復元することは、ほとんど不可能です。それゆえに、タイムスタンプされた文書は著者の意によって改変されることは不可能です。著者もまた発行されたタイムスタンプ証明書を文書の改訂版に適用することはできません。なぜならば、原文書の内容の改変は、たとえ一語または数値データの一位でも、違った文書となり、全く違った指紋値のものにハッシュするからです。代表的なハッシュ値から文書を復元することはできませんが、それにもかかわらず、原文書と主張されているものはこのタイムスタンプ手順で証明されます。というのは原文書表示の真のコピーを包含する受理書は、元のハッシング法を使えば著者の持っている証明書に書かれている、元の数字または同じ連署値に何時でもハッシュするという事実があるからです。

この手順では現在あるどんな決定関数でも使えますが、たとえば、リベスト（「MD4」メッセージ・ダイジェスト・アルゴリズム」、暗号学の進歩—クリプト1990、スプリングー・フェルラー、LNCS、近刊予定）が述べているような方向性ハッシュ関数を引用してここに代入して置きます。この発明の実用においては、かようなハッシング操作は場合によっては著者によって送信中の防衛という著しい利点のためになされます。文書

が暗号文でない形で受理された場合にはタス関数がハッシングするかも知れません。文書の内容と編み込んだ時刻のデータが改変されないようにどのように決定されても、このシステムの信頼性を増すためには、未定世界のメンバーに対して、受理書は、著者ではなく、実際にタス関数によって作られ、示された時刻は正しく、例えば著者と共謀したタス関数が詐欺的に公証したものではないと証明する能力が要しています。

第一の問題に対しては、タス関数は、前述の公開鍵の方法のような、実証できる署名法を用いて、著者へ送信する前にタイムスタンプを付したと証明します。後で、タス関数の公開鍵での解読での署名の検証は、著者と世界全体に対して、証明書はタス関数が作ったものであると証明します。しかしながら、タイムスタンプ自身の真実性の証明は、以下に述べるこの発明の他の部分に依存します。

別の方法では、タス関数は、新しく受理したものを一つ一つその時点までの連署に付け加え、この複合表示に決定関数を用い、即ちハッシングを行い、新しい連署を作って、順次にタイムスタンプした処理の記録を維持します。この連署はハッシング過程によって作られた値で、これが著者に与えられる受理書または証明書に記されて、そこに示されるタイムスタンプを証明するのに役立ちます。後で証明書の検証をするには、著者の時刻受理書とタス関数の記録にあるその直前の連署の値の組合わせに再度ハッシュを行います。その結果著者の証明書に記録の連署値が合えば、著者と全世界に対してその証明書はタス関数で作られたものであると証明します。この結果はまたタイムスタンプの真実性をも証明します。というのは元の受理書に記録の値での元の演算を使わなければ、ハッシング関数によって元の証明書に記録の連署値を作ることはできないからです。

第2図に一般的に書かれているような、この手順の一つの実施例では、著者の世界からタ

ス関数の施設と比較的複雑な文書の流れを利用します。夫々の処理した文書D<sub>1</sub>に対してタス関数はタイムスタンプ受理書を発行し、これには、たとえば、連署受理番号r<sub>1</sub>、著者A<sub>1</sub>の署名番号1D<sub>1</sub>等による記録、文書のハッシュH<sub>1</sub>、その時の時刻t<sub>1</sub>が含まれます。タス関数はこの他に、直前に処理した著者A<sub>1</sub>の文書D<sub>1</sub>の受理データも含め、これによって文書D<sub>1</sub>のタイムスタンプは独自に再立された前の受理時刻t<sub>1</sub>によって「過去」の方向に決定されます。同時に、次に受理した文書D<sub>2</sub>の受理データも、文書D<sub>1</sub>のタイムスタンプを「将来」の方向に決定するために、含められます。複合受理書は今や3つ、あるいは希望によってはそれ以上の、連続したタイムスタンプ受理書の時刻のデータを含み、あるいはそれらの記録部分を含み、タス関数の暗号署名で証明されて、著者A<sub>1</sub>に送ばれます。同時に、D<sub>1</sub>とD<sub>2</sub>の記録表示を含む証明書が著者A<sub>1</sub>に送信されます。このようにして、タス関数によって出されたタイムスタンプ証明書の夫々は連続した時間の中で決定され、配付された多数の関連した証明書を照合すれば順番が通っていれば直ちに判るので、タス関数はどれも偽って発行することはできません。時の流れでの文書のこのような順次の決定は非常に効果的なので、タス関数の署名は実際には必要かもしれません。

第3図に一般的に書かれているような、この手順の第二の実施例では、たとえばタイムスタンプの手順を利用する多数の著者と、広い世界の中にタイムスタンプの仕事を実行するために配付します。タス関数を管理の目的に使ってもよく、あるいは依頼する著者は直接選択したタイムスタンプする著者と連絡してよいわけです。いづれにしても、著者とタス関数の真実でタイムスタンプが文書に付されたのではないという保証が上記の様に必要で、これは少なくとも関数の世界のある部分は実証しようとする著者に買収されないか、そのような著者に暴政の脅威をもちたすという合理的な前提と、特定の文書をタイ

ムスタンプする機関は这个世界から全く無作為に選ばれたという事実の両方で満たされます。著者が著者の自身の選択で共謀しそうな機関を選ぶことが出来ないことは、歴史的な時刻の偽造の可能性を事実上除きます。

この世界の個人のメンバーの中から予定数の機関を選ぶのは、インバグリアッツォ、レビンとルビー（「方向性関数による疑似無作為発生」、第21回STOC会議、12—24ページ、ACM、1989）によって論じられた型の疑似無作為発生機によってです。これに対する最初の値はタイムスタンプされる文書の、ハッシュのような、決定関数であります。値の入力として文書のハッシュや他のこのような関数を与えられると、条件を満たす疑似無作為発生機は一群の機関の署名番号を出力します。この機関の選択は実際上予測できず無作為です。

機関が選ばれると、タイムスタンプは前述のように行われますが、夫々の機関は個性的に受理時刻のデータを受理した文書に付け加え、その結果できたタイムスタンプした別の受理書を機関固有の証明可能な暗号署名で証明し、証明書を著者に返信します。この返信は申請した著者に直接の場合もあり、管理するタス関数を経由する場合もあり、後者の場合にはタス関数が更に証明を付け加えるかも知れません。署名をするという機関と公表された著者の署名番号表は、実際に疑似無作為発生機で選択された機関を利用したことの証明を与えます。本発明の分布した機関を使う実施例は受理書を連署する方法に比べて、タイムスタンプ証明書がより早く発行され、また文書の著者の後での証明は他の著者の証明書が入手できるかどうかにかかりにくい利点があります。

第4図に示される別の実施例では、タス関数が作るタイムスタンプ受理書に、たとえば受理時刻番号r<sub>1</sub>、著者の署名、たとえば署名番号1D<sub>1</sub>等、文書の記録表示、たとえばハッシュH<sub>1</sub>、とその時刻t<sub>1</sub>を含めます。この後タス関数は受理書のこれらのデータ（また

はその代表的な任意の部分)を、その直前に処理した、署名A<sub>1</sub>の文書D<sub>1</sub>の証明書記録番号G<sub>1</sub>に包含し、これによって文書D<sub>2</sub>のタイムスタンプを、独自に確立された時の受理時刻t<sub>2</sub>で限定します。

この複合データの数列(r<sub>2</sub>, ID<sub>2</sub>, H<sub>2</sub>, t<sub>2</sub>, c<sub>2</sub>)はその後ハッシュされて新しい演算値c<sub>2</sub>となり、これが処理番号r<sub>2</sub>とともにタイムスタンプの記録に入れられ、またタイムスタンプ受理番号データとともに証明書記録番号としてA<sub>2</sub>に送信されます。同様に、c<sub>2</sub>と文書D<sub>2</sub>の受理番号のタイムスタンプ演算をハッシュして得られる証明値が署名A<sub>2</sub>に送信されます。このようにして、タイムスタンプが出したタイムスタンプを有した演算証明書の夫々は連続した時の中に確定され、タイムスタンプは決して作ることとは出来ません。何故ならば、前の証明書とハッシュして証明書記録番号を再生しようとすれば矛盾を示すからです。

第5図に示されるような、この発明のより一般的な適用においては、特定の文書の表示、すなわちハッシュは直前の文書の証明書記録番号と単に演算され、この複合表示の決定演算表示、たとえばやはりハッシュ、が次に作られて、この特定の文書の記録上の演算値として保持されます。この増大して行くシリーズの以後の夫々の文書は同様に処理されて記録を拡張し、この記録自身がこのシリーズの中で、もっと広く見れば連続した時の中で、このような文書の夫々が占める位置の信頼できる証明となります。本発明のこの実施例は、たとえば記録がその演算上の数値の文書や記録の順番や連続性を互いに証明できる信頼できる方法を提供します。

本発明の手順の別の例では、署名の記録の中である時間の内に、これは活動の程度によりますがたとえば一日とかそれ以上の間に、作られた(好ましくはハッシュしたりその他の表示の形の)文書の演算をハッシュして、タイムスタンプと証明に併合可能な単一の文書とし

### 発明の記述

本発明の実施例を適用した以下の例で、含まれた手順を更に説明します。説明の便宜上述べられた決定演算は上記のリベストによって記述されたmd4 ハッシング法で、また証明できる署名法はディフィーとヘルマンによって示唆されリベスト等によってアメリカ合衆国特許4,405,829号で実行された公開鍵の方法です。タイムスタンプが実際に適用可能な演算は色々な手に入る演算の中のどれでも良いです。どのような演算が用いられても、何をどの期間使ったかという記録は、受理証明書を後で確認するために維持されなければなりません。更に、手順の説明を簡便にするためと以下に述べるそれ以外の理由の為に、数字の代表的な部分だけを用います。

第2図に示される本発明の受理演算の実施例を最初に考えましょう。この手順はどの様な長さの文書にも使えますが、以下の適切な引用は、ある署名が図2.1で書いてタイムスタンプを希望する文書D<sub>1</sub>を充分に代表するものです。

Time's glory is to calm contending kings,  
To unmask falsehood, and bring truth to light,  
To stamp the seal of time in aged things,  
To wake the morn, and scotch the night,  
To wrong the wronger till he render right;

The Rape of Lucrece

演算で囲まれた任意図2.2で、この文書はmd4演算によって無数の128ビットの数字H<sub>1</sub>にハッシュされますが、この数字H<sub>1</sub>は16進法では

ef6dfdcdb33f3a43d4515a9fb5ce3915

となります。1000人かなる署名の世界の中でシステム認識番号ID<sub>1</sub>が172である

ます。また、偶然然作み発生値の最初の値は、その文書によるだけでなく、時刻の演算や前に受理者が出された文書にもよるかもしれません。別の方法では、一つの記録のなかで署名された人が、常駐する「外部の」機関として、この手順を使ってその組織の文書の演算証明書の記録を維持し、定期的にその時々演算証明書をタイムスタンプに送信します。このようにして、ある記録の演算上の記録の順番が、記録の中でも、また外部的にはタイムスタンプを通じて、確立されます。

また、手順実施例の実行は、原文書表示の受信・ハッシング・演算、タイムスタンプ符号、証明書記録演算の計算と記録、受理証明書の発行という諸段階を直接行う、単一の電算機のプロダムで直ちに自動化されます。

### 図面

本発明の説明には以下の図面を用います：

第1図は本発明による文書タイムスタンプの一般手順の流れ図です。

第2図はこの手順の特定の実施例の流れ図です。

第3図はこの手順のもう一つの特定の実施例の流れ図です。

第4図はタイムスタンプ手順の他の実施例の流れ図です。

第5図は本発明による一般演算手順の流れ図です。

署名A<sub>1</sub>がこの演算番号を付けた文書を図2.3でメッセージ(ID<sub>1</sub>, H<sub>1</sub>)：

172, ef6dfdcdb33f3a43d4515a9fb5ce3915

としてシステムのタイムスタンプする演算として、送信します。

タイムスタンプは、図2.5で、たとえば132という受理時刻番号r<sub>2</sub>と、その時の時刻t<sub>2</sub>の演算を付け加えて、文書D<sub>1</sub>の受理番号を発行します。この時刻の演算は、署名A<sub>1</sub>ができたタイムスタンプ証明書を容易に読めるようにするために、電算機の時計の時刻の標準32ビット表示と文書による演算を、たとえば1990年3月10日グリニッジ平均時16:37:41のように含めるかもしれません。そうすると受理番号は数列(r<sub>2</sub>, t<sub>2</sub>, ID<sub>1</sub>, H<sub>1</sub>)を包含します。

この点で、表示セグメントの数のサイズを前述のように縮らすということを更に考えることが妥当であります。リベスト等によってアメリカ合衆国特許4,405,829号で記述されたように、この例で使われる暗号公開鍵法(この分野では一般に「RSA」署名法として知られています)は、長いメッセージを、一つ一つが暗号化演算資源nを超えない数で表されるブロックに分割することが必要です。夫々のこのブロックはこのRSA法で署名され、送信された後また組み立てられます。それゆえに、RSA法で証明する最終の受理番号が単一のブロックであることを維持しながら、この例で妥当な大きさの数字nを使うためには、受理番号の夫々の演算は代表的な8ビットに縮小されますが、長すぎる数字の場合には普通は最後の8ビットとなり、このビットは16進法では2つのヘキサデシマルの字となります。それで、たとえば、128ビットの文書ハッシュH<sub>1</sub>は最後の8ビット、すなわち0001 0101で表され、これは16進法では15と書かれます。同様に、ID<sub>1</sub>の172は1010 1100で、16進法ではacとなります。

す。実際の計算を行わないで、時刻表示は51と表示されると仮定しましょう。受理番号132は84と表示されます。この点で受理書の数値 ( $r_u$ ,  $t_u$ ,  $ID_u$ ,  $H_u$ ) は  $8451ac15$  となりました。

ここで、直前の文書  $D_{u-1}$  はタス機関によって1990年3月10日16:32:30に ( $t_{u-1}$  の表示は64) に申請

201, d2d67232a61d616f7b87dc148c575174

として処理されたと仮定しましょう。段階27でタス機関はこれらのデータを  $D_u$  に対する受理書数値に加えて、16進法の表示、 $8451ac1564c974$ 、を作ります。この受理書  $R_u$  は今や  $D_u$  に対する時刻と、それ以前には著者  $A_u$  が  $D_u$  が存在したと主張できない時刻  $t_{u-1}$  を確定するデータを含みます。  $A_u$  に対するこの限定は、前の著者  $A_{u-1}$  が時刻証明書  $c_{u-1}$  を保持し、それが  $t_{u-1}$  は著者  $A_{u-2}$  の証明書にあるリンクされた時刻のデータ  $t_{u-2}$  の以後であると限定し、というように、証明が必要なだけ続きます。

タス機関が文書  $D_u$  の受理書を実際に発行したことを確立するために、段階28でタス機関は公開鍵暗号署名法で署名をし、段階29でこの受理書は著者  $A_u$  に送信されて受理証明書または証明書  $c_u$  となります。上のようにして得られたデータを使い、またタス機関は十進法でRSA署名セット

$\langle n, e \rangle = \langle 43200677821428109, 191 \rangle$  (公開)

$\langle n, d \rangle = \langle 43200677821428109, 2940360242249791 \rangle$  (秘密)

を持つとすれば、 $R_u$ ,  $8451ac1564c974$ 、に対する署名付き証明書は

$R^* \bmod n = 39894704664774392$

前例の時と同じく、著者は文書をタス機関へ、普通ハッシュした形で、照番番号を付けた申請として送ります。

172, ef6dfdcdd833f3a43d4515a9fb5ce3915

タス機関は、段階33で、この文書ハッシュ数値を最初の証人の照番番号を作る際として使い、段階35で、選択法

$ID = [md4(\text{値})] \bmod (\text{世界の大さ})$

によって選びます。作られた値ハッシュ:

26f54eae92511dbb5e06e7c2de6e0fcf

は128ビットの数値を表し、その  $\bmod 1000$  が487で、これが最初に選ばれた証人のIDです。次の証人も同様にして選ばれ、この種のハッシュ表示を第2の選択の計算に使って

882653ee04d15bb1f0d604883aa27300b

を得ますが、この  $\bmod 1000$  は571で、これが第2の証人のIDです。この計算を繰り返し、前の種のハッシュを種に使うと最後の証人を598として選びますが、これは  $2fe8768ef3532f15c40acf1341902cle \bmod 1000$  です。

段階37で、タス機関は最初の申請書の写しをこれら3人の証人のそれぞれに送り、段階38で、証人は各側にその時の時刻のステートメントとIDを加え、こうしてできた受理書にRSA暗号署名法で署名して証明し、段階39で証明書を直接著者にまたはタス機関

と計算されるでしょう。著者  $A_u$  がこの証明書  $c_u$  と  $R_u$  の文書のステートメントを受取った時、タス機関の公開鍵を適用すると

$$c_u^* \bmod n = R_u$$

となることから、 $R_u$  は実際に文書のハッシュ  $H_u$  を表示するデータを含んでいると確認され、 $c_u$  が正確であると直ちに確認されます。

この簡単な1リンクの例の手順で作られた証明書は文書  $D_u$  のデータで時間を限定されるので、著者  $A_{u-1}$  に対して、文書  $D_{u-1}$  は文書  $D_u$  の存在のかなり前に時刻を過ぎたのではないという信頼できる証拠を提供します。  $A_u$  の証明書が以後に処理された文書  $D_{u+1}$  からのデータを加えて拡大された時、この証明書は同様に効果的に限定され、 $A_u$  が主張するタイムスタンプを立証します。同じ効果を得る別法としては、 $A_u$  に  $A_{u-1}$  の名を教え、 $A_u$  はその著者から1リンク証明書  $c_{u-1}$  が要請  $H_u$  を含むことを確認できます。この手順は変化する、任意の数の著者のデータを含む受理証明書を発行するようにすることもでき、追加する毎に保証がないという保証の度合いが高まります。

第3図に示される本発明の別の実施例は著者世界の中から無作為に選ばれたメンバーがタス機関 (または証人) となり、すなわち「分布信託」の手順ですが、これは以下のように行われます。実際の適用ではこれらの数はそんなに限定されないのですが、この例では世界は1000人の著者を含み、そのIDは0でない999で、タイムスタンプの真実性を確立するには3人の証人がいれば充分と仮定しましょう。また、この例ではタス機関のサービスを含める前記の変化が実行されています。前の例で用いられたハッシュ関数  $md4$ 、がここでも、任意の段階32で、著者世界から3人の証人を無作為に選ぶ手順をまく決定文書関数の一例として用いられています。

を通じて送信します。後の場合には、タス機関は証明書を一つのファイルにアセンブルして著者に送るかも知れません。証人の選択に当たって無作為性を使うことは個人的な選択を防ぐという事実のために、著者は非協力的な証人がタイムスタンプ証明の前に虚偽の時刻の記入を計画するために選択しようとする危険を避けられます。手順の別法として、著者が直接証人に申請することが許される場合、問題の文書自身が本質的に彼となる証人の無作為性により、著者が文書を知人で協力的な証人に向けてようとする試みを難しくします。できた1枚の証明書は、前述のように署名暗号をして、安心して後の証明に使えます。

図面第4図の段階41のように、タイムスタンプ手順での連続証明書の作成は、著者  $A_u$  が数値文書を照会することから始まります。前述のように、この数値文書は文字数字式テキスト、ビデオ、オーディオ、または確定したデータの他の形のものの数値的な形または表示であるかもしれません。この手順はどのような長さの文書に対しても用いられますが、以下の引用はタイムスタンプしたい文書  $D_u$  を充分に代表します:

...the idea in which affirmation of the world and ethics are contained side by side ... the ethical acceptance of the world and of life, together with the ideals of civilization contained in this concept ... truth has no special time of its own. Its hour is now -- always.

Schweitzer

著者が希望すれば、文書  $D_u$  は安全と送信に必要な帯域幅を減らすために、例えば  $md4$  法で圧縮されます。図面に示された任意の段階42で示されるように、文書は図面の128ビットの形の値  $H_u$  にハッシュされます。これは16進法で

ee2ef3ea60df10cb621c4fb3f8dc34c7

となります。この点で指図しておきますが、この例で用いられる16進法やその他の数値表示は本発明の実施に決定的ではありません。すなわち、与えられた手順によって選ばれたこれらの値のどの部分もまたは他の表示も同様に作用します。

1000人の書き世界の中で署名番号ID<sub>n</sub>が634である書き人A<sub>n</sub>が、段階43でシステムのタス機関に、以下の署名メッセージ(ID<sub>n</sub>, H<sub>n</sub>)で、文書にタイムスタンプを附すよう要請し、文書を送信します:

634. ee2ef3ea60df10cb621c4fb3f8dc34c7

段階44で、タス機関は、受理処理順番号r<sub>n</sub>、例えば1328、とその時の時刻t<sub>n</sub>の表示を加えて文書D<sub>n</sub>の受理書を作ります。この時刻の表示は電算機の時計の時刻の標準2進表示かも知れず、または最終的なタイムスタンプ証明書が容易に読めるように、単に文章の表示で、例えば1991年3月6日グリニジ平均時19:46:28であるかも知れません。この時、受理書は数値(r<sub>n</sub>, t<sub>n</sub>, ID<sub>n</sub>, H<sub>n</sub>)を包含し、これは

1328, 194628GMT06MAR91, 634,  
ee2ef3ea60df10cb621c4fb3f8dc34c7

となります。

本発明によれば、この時のタス機関の記録は、例えば、その時の記録運搬と夫々の受理を次々とハッシュしてできた値の形で、以前の受理処理順での運搬を含みます。かくして、この運搬記録は以下のようにしてできたものです。最初の処理(r<sub>n</sub>=1)では受理書は初期値、すなわちタス機関の記録のハッシュと共にハッシュされて最初の運搬値c<sub>1</sub>を作り、これが最初の処理の証明書の値として使われます。次の処理では、受理書はc<sub>1</sub>と運搬され、

日付: 1991年3月6日  
証明書数: 46f7d75f0fbca95e96fc38472aa28ca1  
この手順はタス機関によって以後のタイムスタンプ要請の即座繰り返されます。A<sub>n-1</sub>からの次の要請がハッシュされた形H<sub>n-1</sub>の文書

201, 882653ee04d511d58bb5e06883aa27300b

で1991年3月6日グリニジ平均時19:57:52に受理されたとすると、複合運搬は

46f7d75f0fbca95e96fc38472aa28ca1,  
1329, 195752GMT06MAR1991, 201,  
882653ee04d511d58bb5e06883aa27300b

となり、A<sub>n-1</sub>に返信される証明書は

処理番号: 1329  
依頼人認識番号: 201  
時刻: 19:57:52グリニジ平均時  
日付: 1991年3月6日  
証明書数: 49bbb1b11d58bb5e06883aa27300b  
となります。

将来、書き人A<sub>n-1</sub>が文書D<sub>n-1</sub>はタス機関によって1991年3月6日19:57:52に受理されたと証明しようと思えば、タス機関の記録が調べられ、直前に処理された1328の運搬受理番号c<sub>1</sub>:

それがハッシュされて第2の証明書記載運搬値c<sub>2</sub>を作り、タス機関のタイムスタンプ要請の全歴史を通じてこれが続きます。

現在の例の直前に文書D<sub>n-1</sub>がタス機関によって、第1327番目の受理要請として処理されて、証明書記載運搬値c<sub>n-1</sub>:

26f54eae92516b1f0d6047c2de6e0fcf

を作ったと仮定しましょう。手順の段階45で、タス機関はこの値とD<sub>n</sub>の受理書を運搬して

26f54eae92516b1f0d6047c2de6e0fcf,  
1328, 194628GMT06MAR91, 634,  
ee2ef3ea60df10cb621c4fb3f8dc34c7

を作ります。この複合表示が、段階46で、タス機関にハッシュされて、新しい証明書記載運搬値c<sub>n</sub>として

46f7d75f0fbca95e96fc38472aa28ca1

を作ります。

この後タス機関はこの値をその記録に加えて、段階47で書き人A<sub>n</sub>にタイムスタンプ証明書を送信します。これには以下の証明書記載運搬値もよく使われます:

処理番号: 1328  
依頼人認識番号: 634  
時刻: 19:46:28グリニジ平均時

46f7d75f0fbca95e96fc38472aa28ca1

が得られます。証明しようとする文書はタス機関に送信された時の形、即ちハッシュに変換され、この値がc<sub>n</sub>やその他のA<sub>n-1</sub>の証明書に記録のデータと運搬されます。問題の文書が本物であれば、複合表示は

46f7d75f0fbca95e96fc38472aa28ca1,  
1329, 195752GMT06MAR1991, 201,  
882653ee04d511d58bb5e06883aa27300b

となり、これをハッシュすると正しい証明書記載運搬値

d9bbb1b11d58bb5e06883aa27300b

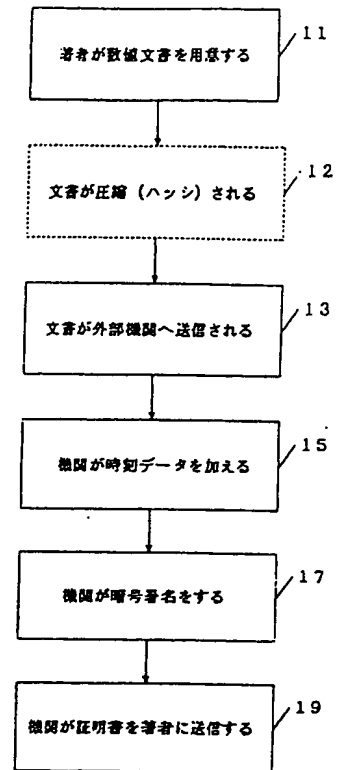
となって、問題の文書はD<sub>n-1</sub>であることが証明されます。さもなければ、改訂された文書はハッシュされると違った値になり、これを要素として含む複合表示をハッシュしたものが処理番号1329の証明書に記録の値と違った証明書記載運搬値となります。

もしもつと証明が必要ならば、例えば文書を改訂した後でc<sub>n-1</sub>も改訂したのではないかというような時には、タス機関の記録から認識されるA<sub>n</sub>の証明書と提出された、即ちハッシュした文書が使われて、その後の、問題となっている証明書値c<sub>n-1</sub>を再計算します。もしその値が正しければD<sub>n-1</sub>は証明されました。別法としては、証明書値c<sub>n-1</sub>は、A<sub>n-2</sub>の証明書値と提出された文書から次の証明書記載運搬値c<sub>n-2</sub>を再計算して証明されます。というのは、もしc<sub>n-1</sub>がD<sub>n-2</sub>を処理番号1330で処理した時のものと同じでなければ、後の文書を変改してc<sub>n-2</sub>と同じ値を得るようになることは不可能だからです。

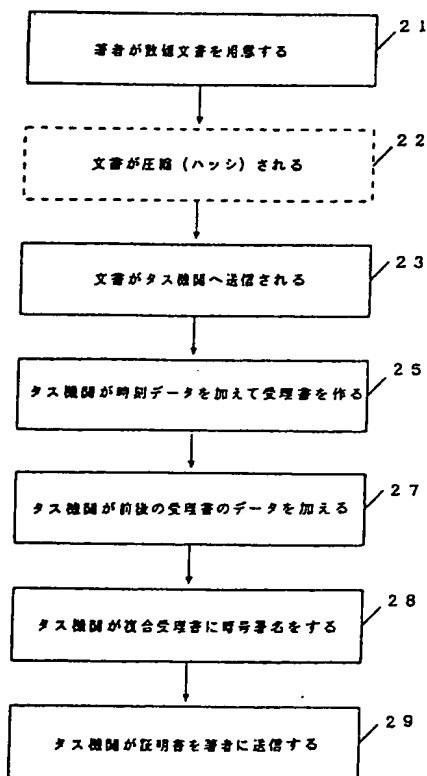
第5図に叙述されているもっと一般的な記録運搬の手順では、拡大するシリーズの文書が、

作られる度に、通関の中またはタス機関で、処理されます。段階51では、決定関数法でハッシュして作られるような、新しい文書の表示が得られ、段階52では、前の文書を処理して得られた現記録値と並べられます。段階53では、この値が計算に記録され、現在の文書に対する新しい記録値を作ります。この値は計算に記録され、証明書に含められるか、あるいは単に処理系に保持されて段階54で提示される次の文書に適用されます。以後の処理段階55、56はこの文書表示に適用され、この手順は新しい文書が来る度に繰り返されます。

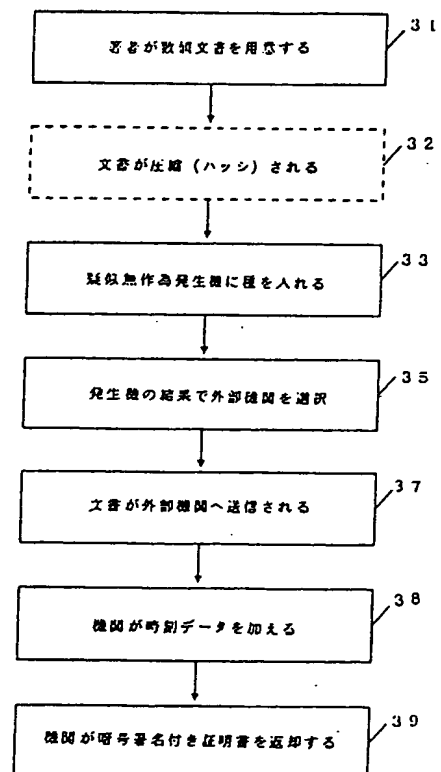
特表平6-501571 (8)



第1図

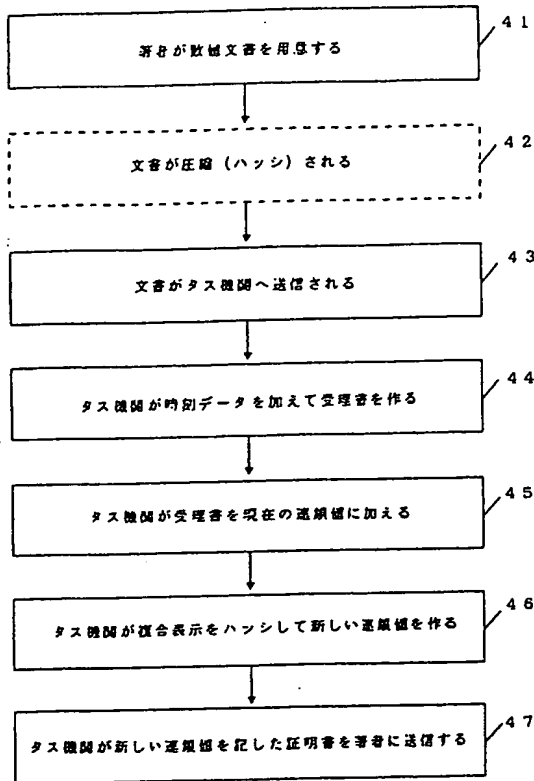


第2図

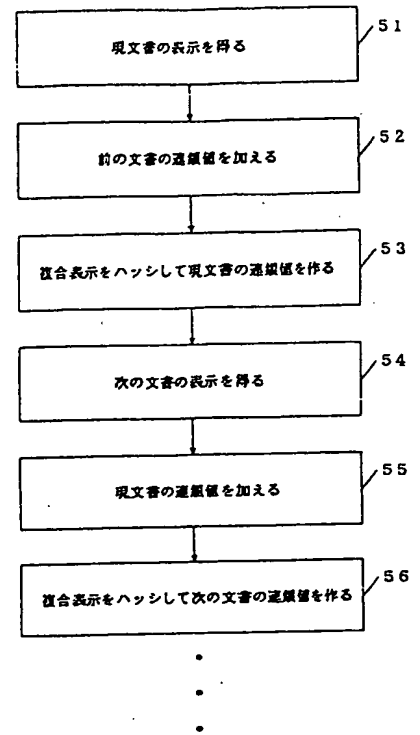


第3図





第4図



第5図

国際調査報告

Report No. 11-116/91

1. CLASSIFICATION OF SUBJECT MATTER		
INT. CL. 3: HQ. 9/00		
U.S. CL. 3: 300/49		
2. FIELD NUMBER		
U.S. 300/4, 3, 3, 30, 49, 50		
3. DOCUMENTS CONSIDERED TO BE RELEVANT		
A	U.S. A. 4,145,568 PUBLISHED 20 MARCH 1979, BRAY.	1-15
A	U.S. A. 4,305,315 PUBLISHED 10 JUNE 1979, MOYAS ET AL.	1-15
4. CERTIFICATION		
Date of the Report: 25 OCTOBER 1991		Date of Making of the International Search Report: 22 NOV 1991
Inventor: ISALS		International Search Report: INTERNATIONAL DIVISION

11/16/91

フロントページの続き

(81)指定国 EP(AT, BE, CH, DE,  
DK, ES, FR, GB, GR, IT, LU, NL, S  
E), CA, JP

(72)発明者 ストーンネット、ウエイクフィールド、スコ  
ット、ジュニア  
アメリカ合衆国、07960 ニュージャージ  
ー州、モリスタウン、ハーディング テラ  
ス 34

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINE(S) OR MARK(S) ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**THIS PAGE BLANK (USPTO)**